PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/32, 12/14, 12/66

A1

(11) International Publication Number: **WO 00/44130**

(43) International Publication Date: 27 July 2000 (27.07.00)

(21) International Application Number: PCT/SE00/00048

(22) International Filing Date: 13 January 2000 (13.01.00)

(30) Priority Data:
9900162–0 20 January 1999 (20.01.99) SE

(71) Applicant *(for all designated States except US)*: NETCOM AB [SE/SE]; P.O. Box 62, S–164 94 Kista (SE).

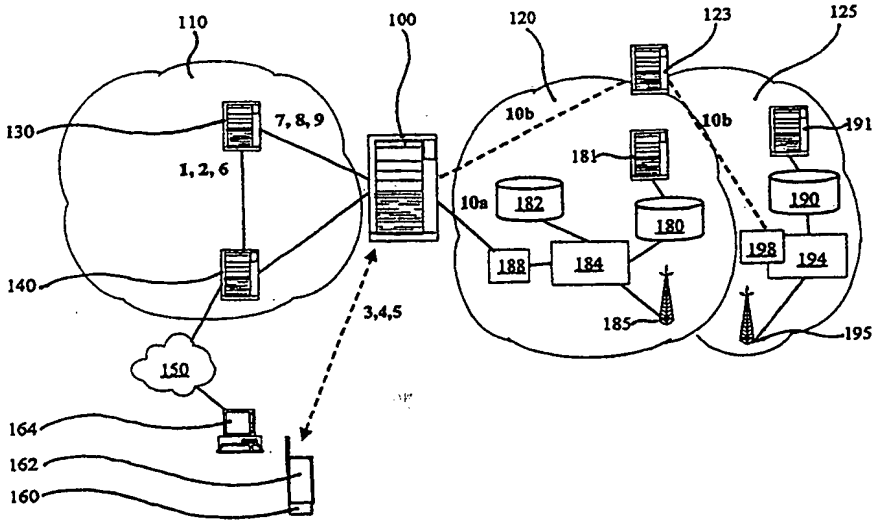
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: BERGGREN, Ulf [SE/LU]; 33, avenue Monterey, L–2163 Luxembourg (LU).

(74) Agent: AWAPATENT AB; P.O. Box 45086, S–104 30 Stockholm (SE).

(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), DM, EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (Utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD, SYSTEM AND ARRANGEMENT FOR PROVIDING SERVICES ON THE INTERNET



(57) Abstract

The present invention relates to a method, a system and a node for providing services on an Internet Protocol based network. These services are based on pre–existing and reliable functionality, in particular an existing user authentication functionality, applied in a digital cellular radio communications network. Such services are to be utilized by servers on the Internet, in particular servers of content providers, that for some reason want to verify the identity of a user, or a customer, accessing the server, for example as a conditional step to using the service of charging a customer, also via the mechanisms of a cellular network.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

A METHOD, SYSTEM AND ARRANGEMENT FOR PROVIDING SERVICES ON THE INTERNET

Technical field of the invention

The present invention relates to a method, a system and a node for providing services on an Internet Protocol based network.

Technical background

The utilization of the Internet has increased rapidly during the last few years and will continue to do so. Two applications on the Internet that are predicted to contribute to this increased utilization are Internet Protocol telephony (IP-telephony) and electronic commerce (E-commerce).

While it is fairly easy for a company or the like to offer its services or products on the Internet, the actual transaction of billing a customer is a bit more complicated and also costly, at least if security aspects are considered.

One way of billing a customer is to bill his credit account number. However, many customers are not willing to transfer their credit account numbers over the Internet, as there is a risk it might fall into wrong hands and be misused. It may not even be allowed to use certain credit cards over the Internet. Someone may be eavesdropping on the Internet or may succeed in manipulating a server on which a company has stored the credit card numbers of its customers. This fear of potential misuse of credit card numbers is probably the major reason why the electronic commerce on the Internet has not increased even further.

Another way for a customer to pay for his purchase is, for example, to transfer the payment from one account to another account within the same bank. However, it is

then necessary for both parties, i.e. the E-commerce company and its customer, to have an account at the specific bank. Alternatively, the accounts of the customer and the E-commerce company are at separate banks. However, in both cases the bank(s) has to provide a system in which security aspects has to be dealt with. Such systems can also include the transferring of a credit card number in an encrypted form from the customer to one of the banks. An example of such a system is the SET-system (Secure Electronic Transactions). One of the major disadvantages with the SET-system, besides being quite complicated, is that it is expensive for an E-commerce company to participate in the system.

Regardless of the system used for offering payment over the Internet, the security will be reflected by the administration routines used for handling payment transaction. Such routines involve the actual payment, but also the identification of the customer. A high security will often require more complicated administrative routines and, thus, a more expensive system to implement and for a company to participate in.

The use of IP-telephony allows a user to make cheap outbound calls in a more or less convenient manner. However, a major disadvantage is that incoming calls can only be received under certain restricted conditions. For example, the user has to be connected to the Internet via a particular Internet Service Provider, or Voice-over-Internet Provider, with which he has a subscription. Also, the user is dependent upon having access to his normal equipment that has the appropriate software being preconfigured in accordance with his subscription. More important, a user is not free to change his physical location, i.e. his Internet Protocol address, if he wishes to be able to receive incoming calls over the Internet. The reason for this is that the calling party, or rather the telecommunications network, does not know

to which voice-over-Internet server the call should be routed.

Summary of the invention

An object of the present invention is to provide a service on an Internet Protocol based network which in a simple and reliable way verifies an end user accessing said network.

Another object of the invention is to provide a content provider on an Internet Protocol based network with a service offering the provider a large potential customer base in which each customer can be verified in a simple and reliable way using said service.

These objects are according to the present invention achieved by a method, a system and a gateway node having the features as defined in the appended claims.

According to a first aspect of the present invention, the above mentioned objects are achieved by a method for providing services on an Internet Protocol based network to which an end user and a server are connected, comprising the steps of: reading an IC card storing subscription information relating to a subscription with an operator of a digital cellular radio communications network, for example a GSM network, at a terminal operated by said end user; requesting a gateway node to verify said end user by means of transmitting from said server to said gateway node a message containing a verification request, said gateway node being connected to said Internet Protocol based network and to either said digital cellular radio communications network or to a network of the same kind as said digital cellular radio communications network; and responding to said verification request with a message from said gateway node to said server, said message being based on a verification of said subscription stored on said IC card, which card for example is a Subscription Identity Module (SIM) card, in accordance with a verification scheme, for

example a GSM authentication scheme, applied by said digital cellular radio communications network.

According to a second aspect of the present invention, the above mentioned objects are achieved by a system for providing services on an Internet Protocol based network to which an end user and a server are connected, said system including: an IC card storing subscriber information relating to a subscription with an operator of a digital cellular radio communications network, for example a GSM network; a terminal operated by said end user and arranged to read said subscriber information from said IC card; and a gateway node interconnecting said Internet Protocol based network with either said digital cellular radio communications network or with a network of the same kind as said digital cellular radio communications network, said node including: receiving means for receiving a verification request from said server to verify said end user; and verification means for performing a verification of said subscription stored on said IC card, which card for example is a Subscription Identity Module (SIM) card, in accordance with a verification scheme, for example a GSM authentication scheme, applied by said digital cellular radio communications network.

According to a second aspect of the present invention, the above mentioned objects are achieved by a A gateway node for providing services on an Internet Protocol based network, to which network a terminal of an end user and a server of a content provider are connected, said terminal being arranged to read an IC card storing subscriber information relating to a subscription with an operator of a digital cellular radio communications network, for example a GSM network, wherein said gateway node interconnects said Internet Protocol based network with either said digital cellular radio communications network or with a network of the same kind as said digital cellular radio communications network, said

gateway node having the features as defined above in connection with the second aspect of the invention.

Thus, the present invention is based on the idea of providing services on the Internet that are based on pre-existing and reliable functionality, in particular an existing user authentication functionality, applied in a digital cellular radio communications network. Such services are to be utilized by servers on the Internet, in particular servers of content providers, that for some reason want to verify the identity of a user, or a customer, accessing the server.

Using already existing and reliable verification functionality provided by a digital cellular radio communications network for verifying a user on the Internet, makes the verification of the user simple and inexpensive. There is no need for a content provider, or any other party, to design, provide and maintain a new, complicated and costly system for enabling a reliable way of verifying users accessing servers on the Internet.

The advantages of the present invention are achieved irrespective of to what extent the verification functionality is actually run by the cellular network or if a part of the functionality is implemented by the inventive gateway node on basis of the principles used by the cellular network.

According to an embodiment of the invention, said terminal operated by said end user is a computer, for example a personal computer, arranged to read a SIM card via a SIM card reader connected to the computer. The computer is also used by the user for accessing the Internet. The computer and the gateway node are arranged to communicate over the Internet using standard GSM signalling mechanisms. This communication includes exchanging GSM authentication parameters in the process of verifying the subscriber of the SIM card. This verification is performed in accordance with the verification, or authentication, normally applied in a GSM network. For this

reason, the gateway node includes a database implementing GSM VLR functionality as well as other necessary means and software for communicating with the GSM network, to which the subscription is associated, in order to make use of the charging and location update procedures provided in the GSM network.

According to another embodiment of the invention, said terminal operated by said end user is a mobile station comprised of a mobile equipment reading a SIM card. By using the mobile station for making a GSM call to said gateway node, a temporary verification code is assigned to the GSM mobile station number by the gateway node as a result of reception of the call and, thus, as a result of the calling subscriber having been authenticated by the GSM network. This number and code can be utilized by the user when communicating with a server of a content provider, using the normal computer equipment used for accessing the Internet, in order for the user to finally be verified by the server of the content provider. Thus, there is no need for any additional user equipment or software having to be distributed and maintained at the user premises or within the terminal used for accessing the Internet. As an alternative to dialling a public telephone number, the mobile station establish a communication with the gateway node by means of transmitting a SMS (Short Message Service) message, in which case a call is made from the gateway node back to the GSM mobile station in order to transfer the temporary verification code.

According to the invention, an operator of the gateway node is able to provide services relating to customer authentication and invoicing of customers to any content provider on the Internet. It is also possible to provide a customer locating service to a voice-over-Internet content provider. All the Internet user, or customer, needs is a GSM subscription with which he can roam outside his HPLMN. He also needs a mobile equipment, alternatively a

SIM card reader connected to a terminal, such as a personal computer, together with a specific software stored on the computer for handling GSM signalling over the Internet. Of course, the user is assumed to have the tools necessary for accessing the Internet (such as a PC or the like, a modem and an Internet subscription with an Internet Service Provider).

In addition, by providing a service on the Internet which is based on existing charging functionality of a digital cellular radio communications network, for example a GSM network, the implementation of a secure and effective way to charge an end user is greatly simplified. According to the invention, charging records are produced and fed into the invoicing mechanism of the cellular network.

It should be noted that the described existing verification and charging functionalities and schemes, described in the present invention, is not restricted to those of a GSM network, but may be provided by any digital cellular radio communications network having functionalities or schemes that correspond to those of a GSM network.

Thus, the invention offers a secure and simple way of verifying and charging an end user on the Internet. Provided that the end user has a subscription with cellular network of the same kind as the one to which the gateway node according to the invention is connected, any server connected to the Internet can use the open interface provided by the gateway node to verify and/or charge the end user that accesses the server. Of course, the end user has to have his IC card storing his subscriber information connected to the IC card reader of his terminal, or, in accordance with another embodiment, to his mobile equipment (ME).

Thus, any content provider on the Internet can arrange for its server to use the services provided by the present invention. In the context of the present

invention, a content provider is anyone providing a service on the Internet. Such services include, inter alia, electronic commerce, IP telephony and the actual Internet access itself.

Moreover, a content provider can target all customers having a subscription with an operator of a cellular network, such as a GSM network, since the roaming principles of the cellular network allows for operators to offer services to other operators' customers. In this way a great number of potential customers is opened to an Internet application using the services provided by the present invention.

A great advantage for a voice-over-Internet provider that uses the services provided by the system, and the gateway node, is that he can offer his customers not only to make outbound calls, but also to receive calls made to the customers GSM Mobile Station Integrated Service Digital Network (MSISDN) number. This is irrespectively of which physical address the customer is connected to. Thus, the invention provides fixed access roaming, or mobility to Internet telephony customers.

Another advantage with the present invention is the ability to provide a very fast service deployment.

The gateway node according to the invention is preferably operated by an operator providing verification, charging and mobility services on the Internet, i.e. an Internet Charging and Mobility Provider. Moreover, the gateway node should be interpreted as a logical node, which can be realised as either one single physical unit or as a number of physical separate units, or sub-nodes, among which the functionality of the logical gateway node is distributed.

Brief description of the drawings

Further features and advantages of the present invention will become more apparent from the following detailed description of specific embodiments of the

invention when taken in conjunction with the accompanying drawings in which like reference characters identify correspondingly throughout and wherein:

Fig. 1 shows a system and its operation in accordance with an embodiment of the present invention;

Fig. 2 shows a system and its operation in accordance with another embodiment of the present invention;

Fig. 3 shows a system and its operation in accordance with yet another embodiment of the present invention;

Fig. 4 schematically shows a gateway node included in the embodiment described with reference to Fig. 1; and

Fig. 5 schematically shows a gateway node included in the embodiments described with reference to Fig. 2 and Fig. 3.

Detailed description of preferred embodiments

Fig. 1 shows an exemplified system and its operation in accordance with an embodiment of the present invention. In Fig. 1, a gateway node 100 is connected to an Internet Protocol based network 110, such as the Internet, and a digital cellular radio communications network 120. Connected to the Internet 110 is a server 130 of a content provider, in this case an E-commerce provider selling products or services over the Internet. Another content provider, being an Internet Service Provider (ISP), has an access server 140 connected to the Internet as well as to a switched telecommunications network 150.

An IC card 160 stores subscriber information relating to a subscription with an operator of a digital cellular radio communications network. This cellular network, provided by the subscriber's home operator, is called a Home Public Land Mobile Network (HPLMN) and corresponds in Fig. 1 to either the cellular network 120, to which the gateway node is connected, or to a cellular network 125, which the gateway node is connected to via intermediate telecommunications facilities. Of course,

the connection between the gateway node 100 and the cellular network 120 may also, alternatively, be over intermediate communications facilities, such as a switched telecommunications network in the form of a Public Switched Telephone Network. Thus, in Fig. 1, one of the cellular networks 120 and 125 is the HPLMN of the subscription stored on the IC card 160. In case the cellular network 125 is the HPLMN, the cellular network 120 constitutes a Visited Public Land Mobile Network (VPLMN). The IC card 160 is received and read by a terminal 162, which terminal is a mobile station operated by an end user. The end user uses the mobile station 162 to access the gateway node via one of the cellular networks, i.e. 120 or 125.

To access the Internet 110, the end user operates a second terminal 164, preferably a Personal Computer (PC). This Internet access is accomplished, for example, via a modem connected to the PC, the telecommunications network 150 and a modem pool connected to the access server 140 at the premises of the ISP.

In Fig. 1 the digital cellular radio communications networks 120 and 125 are exemplified with GSM mobile communication networks (Global System for Mobile communication). Since the architecture, and operational aspects, of GSM are well known to persons skilled in the art, only those aspects of GSM which are of direct relevance to the embodiments of the present invention will from hereon be described.

A GSM network typically includes a Home Location Register (HLR) 180, an Authentication Centre (AUC) 181, a Visiting Location Register (VLR) 182, one or more Mobile service Switching Centres (MSC) 184, a number of Base Stations (BS) 185, and means 188 for implementing a Billing Customer Administration (BCA) functionality, as indicated in the GSM network 120. The GSM network 125 has the corresponding elements, i.e. HLR 190, AUC 191, MSC 194, BS 195 and BCA 198. The combination HLR and AUC

keeps all information relating to the GSM subscribers of an operator's GSM network and also knows the last location of any one of these subscribers.

The VLR 182, which often is integrated with an MSC 184 and its functions, is a register storing subscriber information received from the HLR 180 and relating to subscriber which have roamed to the area covered by the particular VLR 182, which area is a part of the total area covered by the GSM network 120. The BCA 188 is used by the operator of the GSM network 120 when billing its subscribers. The operation and functioning of an MSC 184 and a BS 185, as well as other elements and their functions, are well known to a person skilled in the art and not of relevance in the context of the present invention.

As the cellular network with which the user has a subscription is a GSM network, the IC card 160 will be a SIM (Subscriber Identity Module) card. The SIM card 160 uniquely identifies a GSM subscriber to the network and holds information and algorithms for subscriber authentication and encryption, as is well known to a person skilled in the art.

The following is a description of the operation of the system, when providing services on the Internet, as depicted in Fig. 1. The activities described below have been numbered and each number indicated in Fig. 1 in order to more clearly illustrate which element(s) that is/are involved in a certain activity.

In step 1, a user having access to the Internet 110 via its ISP contacts a server 130 at a content provider site, for example an E-commerce provider, and decides to make a purchase of some sort. In step 2, the user chooses "GSM" as charging method, possibly among a number of choices of charging methods, and is then asked by the server 130 to enter his mobile station number, or an alias corresponding to this number, and a password. The mobile station number, possibly via said alias, uniquely identifies the user's subscription in the Public Switched

Telephone Network (PSTN) numbering plan with an operator of a cellular network. Since the cellular network is a GSM network, the mobile station number would be a GSM Mobile Station Integrated Service Digital Network (MSISDN) number.

The password is obtained by the user from the gateway node 100 in step 3. This is accomplished by establishing a communication from the GSM mobile station to the gateway node, for example by dialling a public telephone number from the mobile station 162, and thereby calling the gateway node 100 via the users HPLMN, or if the user is roaming, via a VPLMN. In step 4 the gateway node 100 answers the call and prompts the user to enter a special PIN (Personal Identity Number) code, which code was assigned to the user by the operator of the gateway node 100 when the user started to subscribe for the services offered by the gateway node operator. The gateway node examines the calling A-subscriber number in order to check that the number is a number of a subscriber in a GSM network. The mere fact that the subscriber has been able to call the gateway node 100 using his GSM subscription is a receipt on that the subscriber has been authenticated by the GSM network 120 or 125. The gateway node could also, to add extra security to the verification procedure, disconnect the GSM connection and initiate a new connection with the GSM subscriber. As an alternative to dialling a public telephone number, the subscriber sends an SMS (Short Message Service) to the gateway node, which also is a receipt on that the subscriber has been authenticated by the GSM network. The verification of the subscriber performed by the gateway node 100 is thus based on the authentication performed by the GSM network 120 or 125, after which authentication a number of additional measures are taken by the gateway node as further described below. If the special PIN code received from the user is correct, i.e. if it matches the user's MSISDN recorded by the gateway node as the user

call was received, the gateway node 100, in step 5, assigns another PIN code, being a Temporary PIN code (TPIN), to the user. The TPIN is associated with the MSISDN of the user and stored together with the MSISDN in the gateway node 100 for later use, as well as being transmitted to the user's mobile station. In the SMS case described above, the TPIN is transmitted to the user's mobile station with in a call from the gateway node to the mobile station. The TPIN is temporary in the sense that it only is valid for a short time and can only be used at one occasion by the user after it has been allocated to him.

The TPIN received by the user via his mobile station 162 is then in step 6 used in the Internet session with the Internet server 130 being accessed using the second terminal 164, in this case a server of an E-commerce provider. The user enters, using the second terminal 164, his MSISDN as user id and the received TPIN code as password, all in accordance with the prompting of the server 130. In step 7, the server 130 includes the MSISDN and the TPIN received from the user in a verification request transmitted over the Internet 110 to the gateway node 100. In step 8, the gateway node 100 extracts the MSISDN from the verification request, finds the corresponding MSISDN and its previously associated TPIN stored within the gateway node, and checks if the previously stored TPIN is equal to the TPIN extracted from the received verification request. If the TPIN codes are found to be matching, the verification of the user at the gateway node is completed and a response is transmitted to the server 130 indicating a confirmation, or possibly a rejection, to the verification request.

In step 9, following a received notification that the user has been verified by the gateway node 100, the server 130 transmits a charging request including the verified MSISDN to the gateway node requesting the node to charge that particular MSISDN, either by using usage

based charging or by charging the subscriber a certain amount. In the following step, the gateway node 100 charges the subscription having the particular MSISDN by either producing a Call Detail Record (CDR), referenced in Fig. 1 as step 10a, or a Transfer of Account Procedure Record (TAP), referenced as step 10b. In case a certain amount should be charged, this charging step may preferably involve checking an agreed credit level for the particular MSISDN, in which case only amounts lower than said credit level will be accepted by the gateway node when performing the service of charging the subscriber. This credit level is either stored in the gateway node or received, upon request from the node, from the GSM network.

If the HPLMN of the subscription having the particular MSISDN is the GSM network 120, a CDR record is generated by the gateway node 100 and transmitted over the GSM network 120 to the Billing Customer Administration system 188 of that network, this is indicated as step 10a. If, on the other hand, the subscriber has been roaming and the HPLMN of the subscription is the GSM network 125, in which case the GSM network 120 is a VPLMN, a TAP like record is generated by the gateway node in accordance with the TAP standard and transmitted to a clearing house 123. A clearing house is a unit that receives TAP records from operators and that clears these the operators' internal invoices for roaming customers. Thus, the internal invoice of GSM network 120 will be cleared and the BCA of the GSM network 125 receives information from the clearing house based on which it will bill its own subscriber. Depending upon whether or not the gateway node generates one of these CDR and TAP like records, the node will transmit a rejection or a confirmation back to server 130 as a result to said charging request.

The gateway node 100 will later be further described with reference to Fig. 4.

It should be understood that the system operation described above also is suited in a situation where the Internet Service Provider, ISP, wishes to verify and charge its customers for the service of providing Internet access using the verification and charging procedures provided by the GSM network, rather than having to administrate its own billing system. In this case, the server transmitting requests for verification and charging to the gateway node will be the access server 140 belonging to the ISP rather than the server of the E-commerce provider as described above.

In Fig. 2 another embodiment of the system and its operation according to the present invention is schematically illustrated. The basic system configuration corresponds to that of Fig. 1. All elements in Fig. 2 that have been assigned the same reference numerals as in Fig. 1 are identical to and have the same operation as the corresponding element described with reference to Fig. 1. Thus, only operational aspects that differ from the operations described with reference to Fig. 1, as well as additional aspects that are relevant to the embodiment illustrated by Fig. 2, will be described below.

Again, the digital cellular radio communications networks 120 and 125 are exemplified with GSM networks. The GSM network 120 is the HPLMN network of the subscription stored on the IC card 160, the other GSM network 125 is a VPLMN network. In the embodiment described with reference to Fig. 2, the IC card 160, which again is a SIM card, is inserted and read by a SIM card reader 261 connected to a terminal 262. In this embodiment the terminal 262 is a stationary computer, for example a Personal Computer (PC). The PC executes a software application which communicates with the SIM card via the SIM card reader, with the user via a PC screen and with the gateway node 200 via an Internet Protocol connection over the Internet 110.

The gateway node 200 has an operation and an internal structure which differs from that of the gateway node referred to in Fig. 1. In the embodiment of Fig. 2, the gateway node 200 includes a database in the form of a GSM VLR as well as some parts of the functionality normally found in a GSM MSC/VLR in a GSM system. The operation of the gateway node and its interaction with the GSM networks 120 and 125 is described below. The internal structure of the gateway node itself is more clearly described with reference to Fig. 5.

In step 1, a user having access to the Internet via its ISP contacts a server 230 of a content provider, for example an E-commerce provider, and decides to make a purchase of some sort, the user chooses "GSM" as charging method. The server 230 then in step 2 transmits a verification request to the gateway node 200. Included in this verification request is an Internet Protocol address associated with the terminal 262 operated by the user.

In step 3, the gateway node 200 requests the terminal 262 at the previously received IP address to perform a registration request. A registration request is then in step 4 transmitted by the terminal 262 over the Internet as an IP message to the gateway node 200. The transmitted registration request is the same kind as the one a mobile station transmits when switched on or when roaming into a new geographical area, and includes subscriber information read from said SIM card 160. In step 5, the gateway node accesses the VLR database included in the gateway node in order to retrieve GSM authentication parameters, i.e. verification parameters, associated with the subscription of the SIM card 160, which subscription was derived from said received subscriber information. If the subscriber has been roaming, i.e. if the user having his SIM card 160 connected to a PC 262 for some reason, for example by connecting to a new PC or by a new IP address being associated with the PC currently used, is associated with a different IP address than the one the user

previously used, or if it is otherwise deemed necessary, the gateway node will initiate a GSM standardised location update routine to be performed, indicated as step 6. This location update involves registering the subscriber in the HLR 180 of the HPLMN GSM network 125 as being present in the area covered by the gateway node 200, or rather by its included VLR. The location update routine further involves the transferring of GSM authentication parameters from the HLR 180/AUC 181 to the gateway node 200 for storage in the included VLR. These parameters received and stored at the gateway node are then used in the following step 7, which step involves exchanging authentication parameters between the gateway node 200 and the terminal 262. If this GSM standardised way of exchanging authentication parameters results in that the subscription is authenticated, the verification of the user at the gateway node 200 is completed and a response is transmitted to the server 230, in step 8, indicating a confirmation of said verification request previously received from the server 230. Of course, a verification request could, alternatively, result in a rejection transmitted to the server.

In step 9, the server 230 transmits a charging request to the gateway node 200 for charging the verified subscription for a product or service being purchased. The gateway node charges the subscription in a GSM standardised way by either producing a CDR record or a TAP like record. The generation of these records and the charging procedure is performed in accordance with the GSM standard and in accordance with what has been previously described with reference to Fig. 1. Also, as previously described with reference to Fig. 1, a response to said charging request will be transferred from the gateway node 200 to the server 230.

Again, as described with reference to Fig. 1, the operation described above is also applicable when it is

the access server 240 of the ISP that requests the gateway node to verify and charge a subscription.

It should be noted that a verification request for verification of a user, as well as the request to charge a user, at a certain IP address can be requested by the server 230 of a content provider at any time. If the server is a server of an ISP, that is if server 230 utilizing the services provided by the gateway node is one and the same server as the Internet access server 240 of the ISP, this one server would transmit the verification request to the gateway node at the start of the Internet access session, which request at a later stage is followed by a charging request to the gateway node from the Internet access server. Thus, the subscription of the user is verified using the GSM authentication scheme, and charged for the Internet surfing using the GSM invoicing scheme. A server of an E-commerce provider could transmit the verification request as the customer enters the E-commerce site, or just before purchasing, i.e. before the transmission of the charging request. The time chosen for transmitting a verification request, as well as a charging request, is entirely up to the Internet content provider.

In Fig. 3 yet another embodiment of the present invention is schematically illustrated. This embodiment differs from the one described with reference to Fig. 2 in that the server using the services provided by the gateway node 200 and the server providing a user access to the Internet 110 is one and the same server, namely a server 330 of a voice-over-Internet provider. Again, all elements in Fig. 3 being identical and having the same operation as those described with reference to Figs. 1 and 2 have been assigned the same reference numerals as in Figs. 1 and 2.

Fig. 3 shows how a terminal 262, operated by a user and referred to as an A-subscriber, makes an Internet telephone call to a B-subscriber 360. The B-subscriber is

connected to a gateway server 370 on the Internet via a General Switched Telecommunications Network 350, the gateway server 370 converts voice traffic from a circuit switched network 350 to a packet switched network 110. The voice-over-Internet server 330 communicates with the gateway server 370 over an Internet session.

The operation for verifying the user and for charging the user are almost identical to the embodiment of Fig. 2. The difference is that as the user operating the terminal 262 connects to the voice-over-Internet server 330, the server will automatically send a verification request to the gateway node 200. The verification of the user, i.e. the authentication of the GSM subscription, is performed as described with reference to Fig. 2. The server 330 transmits a charging request whenever it is convenient and charging of the GSM subscription is performed as described in the two previous embodiments.

The use of the GSM principles for verification of the GSM subscription and, thus, the registration and GSM location update procedure described in connection with Fig. 2 enables the server 330 to provide its customers with the service of receiving incoming Internet telephony calls, regardless of the location of the user. This is possible since the HLR 180 of the subscribers GSM HPLMN network has registered the visited VLR/MSC address, in this case the gateway node 200, for a particular subscriber. The HLR requests the visited gateway node to return a MSRN (Mobile Station Roaming Number) which is used to route an incoming call to the correct gateway node visited by the subscriber. The MSRN is then used in setting up a call to the user when the user's GSM Mobile Station Number is dialled in any international GSTN network connected to the user's GSM HPLMN network, all in accordance with the recommendations for GSM. The gateway node 200 will establish an Internet session with the IP address of the user's terminal 262, provided that the

user is present on a public IP address in the global IP address scheme.

Fig. 4 schematically shows an exemplifying gateway node included in the embodiment described with reference to Fig. 1. The node includes a processor 400, receiving means 410, verification means 420 and 425, and charging means 430.

The receiving means 410 is implemented as a standardised TCP/IP stack executed by the processor 400 and receives IP messages including verification requests and charging requests from servers on the IP network.

The verification means 420 and 425 includes first means for associating a TPIN with a GSM MSISDN number of a mobile station from which a call is received, second means for storing said TPIN together with said MSISDN number and third means for checking the correspondence between a code received with a MSISDN number in a verification request and a TPIN stored together with the same MSISDN number by the second means. The first and second means, indicated with reference numeral 420 are easily implemented as software routines by a person with ordinary skill in programming and the second means, indicated with reference numeral 425, is implemented as any kind of storage means, such as a table in a database.

The charging means 430 comprises software routines for generating CDR records and TAP like records communicated to a GSM network and a clearinghouse, respectively.

Fig. 5 schematically shows an exemplifying gateway node included in the embodiments described with reference to Fig. 2 and Fig. 3. The node includes a processor 500, receiving means 510, verification means 520, a database 527, charging means 530, first communication means 540, second communication means 550 and registration means 560. The receiving means 510 and charging means 530 correspond to the previously described receiving means and charging means described in Fig. 4.

The verifying procedure performed by the gateway node of Fig. 5 involves the first and second communication means, 540 and 550, respectively, the verification means 520, the database 527 and the registration means 560. The first communication means 540 comprises a applicable parts of BSSAP (Base Station System Application Part) implemented on top of the TCP/IP stack and handles the GSM signalling over the Internet towards a user terminal. These first means 540 also includes a software routine for requesting a user terminal at a particular IP address to transfer subscriber information read from the SIM card connected to the user terminal. The user terminal interconnects the SIM card and the Internet by means of a SIM card reader, and transmits the read subscriber information using corresponding communication means at the terminal, also implemented as BSSAP on top of an TCP/IP stack. The above described first communication means 540 of the gateway node and communication means of the terminal are utilized when exchanging GSM authentication parameters during verification of the SIM card subscription. This exchange of authentication parameters either occurs as a result of a request from the gateway node to the terminal, or as a result of an initiative from the terminal.

The database 527, stores GSM authentication parameters associated with different subscribers. The database handles the functionality normally provided by a GSM VLR. In case these parameters need to be transferred from the HLR of the subscriber's HPLMN network, the registration means 560 implements the necessary software routine for using said second communication means 550, which means implements the GSM standardised Mobile Application Part (MAP) routines for signalling with the GSM network, to initiate a GSM location update routine using appropriate signalling towards the GSM HPLMN network. The verification means 520 includes additional software for co-ordinating all the above described means involved in

the verification procedure, as well as software for, for example, checking any possible credit levels associated with different subscribers.

The previous descriptions of the preferred embodiments are provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without the use of any inventive facility.

CLAIMS

1. A method for providing services on an Internet Protocol based network to which an end user and a server are connected, comprising the steps of:

reading an IC card storing subscription information relating to a subscription with an operator of a digital cellular radio communications network, for example a GSM network, at a terminal operated by said end user;

requesting a gateway node to verify said end user by means of transmitting from said server to said gateway node a message containing a verification request, said gateway node being connected to said Internet Protocol based network and to either said digital cellular radio communications network or to a network of the same kind as said digital cellular radio communications network; and

responding to said verification request with a message from said gateway node to said server, said message being based on a verification of said subscription stored on said IC card, which card for example is a Subscription Identity Module (SIM) card, in accordance with a verification scheme, for example a GSM authentication scheme, applied by said digital cellular radio communications network.

2. A method as claimed in claim 1, comprising the further steps of:

requesting said gateway node to charge said end user by means of transmitting from said server to said gateway node a message containing a charging request; and

performing, at said gateway node, a charging procedure for charging said subscription in accordance with a charging scheme applied by said digital cellular radio communications network, for example a charging scheme included in a GSM invoicing scheme.

3. A method as claimed in claim 2, comprising requesting, from said gateway node, said end user to confirm said charging procedure prior to executing the same.

4. A method as claimed in claim 2 or 3, wherein said charging procedure involves generating a charging record, for example a Call Detail Record (CDR), or generating charging information, for example a Transfer of Account Procedure (TAP) like record, for use by a charging procedure of a remote digital cellular radio communications network with which said end user has said subscription.

5. A method as claimed in any one of claims 1 - 4, wherein said terminal of said user is a mobile station, and wherein said verification of said IC card includes the steps of:

receiving at said gateway node a call, or a short message, from a said mobile station via said digital cellular radio communications network;

associating at said gateway node a temporary verification code to a mobile station number of the mobile station having established a connection with the gateway node;

storing at said gateway node said temporary verification code together with said mobile station number;

transmitting said temporary verification code to the mobile station which initiated the connection; and

checking that a received verification code associated with a mobile station number, both of which are received in said verification request from said server, is identical to the temporary verification code previously stored together with said mobile station number.

6. A method as claimed in claim 5, comprising incorporating at said server said mobile station number and

said verification code in said verification request transmitted to said gateway node.

7. A method as claimed in claim 5 or 6, comprising the step of:

establishing a communication with said gateway node via said digital cellular radio communications network using said mobile station by means of either calling a public telephone number or by transmitting a short message;

receiving at said mobile station a temporary verification code as a response to said step of establishing a communication;

entering said mobile station number and said verification code into a second terminal, which terminal is used by said end user to access said Internet Protocol based network; and

transmitting said mobile station number and said verification code to said server.

8. A method as claimed in any one of claims 5 - 7, wherein said mobile station number uniquely identifies said subscription in the public switched telephone network numbering plan, for example a GSM Mobile Station Integrated Services Digital Network (MSISDN) number.

9. A method as claimed in any one of claims 1 - 4, wherein said terminal is a personal computer with which said end user accesses said Internet Protocol based network, said terminal being associated with an Internet Protocol address.

10. A method as claimed in claim 9, wherein said verification request includes said Internet Protocol address, which address is used by said gateway node for requesting said terminal to transfer said subscriber information of said IC card to the gateway node.

11. A method as claimed in any one of claims 1 - 4, 9 or 10, wherein said verification of said IC card includes the steps of:

accessing verification parameters associated with said subscription, for example GSM authentication parameters, stored in a database, for example a GSM Visitor Location Register, included in said gateway node; and

exchanging verification parameters between said gateway node and said terminal.

12. A method as claimed in claim 10, wherein said transfer of said subscriber information to the gateway node is performed as a registration request transmitted from said terminal, and wherein said method comprises registering, at said gateway node, said subscription in accordance with a registration scheme applied by said digital cellular radio communications network, for example a GSM location update scheme.

13. A method as claimed in claim 12, wherein said registering comprises:

searching a database for data matching said subscriber information;

requesting, if matching data is not found during said searching step or if it is otherwise deemed necessary, the digital cellular radio communications network with which said end user has a subscription to perform an update registration procedure based on said subscriber information;

storing data, received from the digital cellular radio communications network as a response to said requesting step, in said database; and

performing said verification of said IC card using said data stored in said database.

14. A method as claimed in any one of the preceding claims, wherein said server is a server of a content provider on said Internet Protocol based network.

15. A method as claimed in claim 14, wherein said content provider is either an E-commerce provider, a Voice-over-Internet provider or an Internet Service Provider.

16. A system for providing services on an Internet Protocol based network to which an end user and a server are connected, said system including:

an IC card storing subscriber information relating to a subscription with an operator of a digital cellular radio communications network, for example a GSM network;

a terminal operated by said end user and arranged to read said subscriber information from said IC card; and

a gateway node interconnecting said Internet Protocol based network with either said digital cellular radio communications network or with a network of the same kind as said digital cellular radio communications network, said node including:

receiving means for receiving a verification request from said server to verify said end user; and

verification means for performing a verification of said subscription stored on said IC card, which card for example is a Subscription Identity Module (SIM) card, in accordance with a verification scheme, for example a GSM authentication scheme, applied by said digital cellular radio communications network.

17. A system as claimed in claim 16, wherein:

said receiving means of said node is further arranged for receiving a charging request from said server to charge said end user; and

said node further includes charging means for charging said subscription in accordance with a charging

scheme applied by said digital cellular radio communications network, for example a charging scheme included in a GSM invoicing scheme.

18. A system as claimed in claim 17, wherein said charging means are further for generating a charging record, for example a Call Detail Record (CDR), or for generating charging information, for example a Transfer of Account Procedure (TAP) like record, for use by a charging procedure of a remote digital cellular radio communications network with which said end user has said subscription.

19. A system as claimed in any one of claims 16 - 18, wherein said terminal is a mobile equipment forming a mobile station together with said IC card.

20. A system as claimed in claim 19, wherein said verification means include:

first means for associating a temporary verification code to a mobile station number of said mobile station from which a call is received;

second means for storing said temporary verification code together with said mobile station number; and

third means for checking whether a verification code, received with a mobile station number in said verification request, is identical to the temporary verification code being stored together with said mobile station number.

21. A system as claimed in claims 20, including a second terminal, with which said end user accesses said Internet Protocol based network, arranged for receiving said the temporary verification code and said mobile station number.

22. A system as claimed in claim 20 or 21, wherein said mobile station number uniquely identifies said subscription in the public switched telephone network numbering plan, for example a GSM Mobile Station Integrated Services Digital Network (MSISDN) number.

23. A system as claimed in any one of claims 16 - 18, wherein said terminal is a personal computer which is connected to a card reader for reading said IC card, said terminal being associated with an Internet Protocol address and used by said end user to access said Internet Protocol based network.

24. A system as claimed in any one claims 16 - 18 or 23, wherein said gateway node includes a database in which verification parameters associated with subscriptions are stored, said parameters being accessed during said verification of said end user.

25. A system as claimed in any one of claims 16 - 18, 23 or 24, wherein said gateway node includes first communication means for requesting said terminal to transfer said subscriber information of said IC card, and wherein said terminal includes communication means for transmitting said subscriber information read from said IC card to said gateway node.

26. A system as claimed in any one of claims 23 - 25, wherein said gateway node and said terminal are arranged to exchange verification parameters during said verification of said end user.

27. A system as claimed in any one of claims 23 - 26, wherein said terminal is arranged to transmit said subscriber information to said gateway node, in response to a request from the gateway node, as part of a registration request, and wherein said gateway node includes

registration means for performing a registration of said end user in accordance with a registration scheme applied by said digital cellular radio communications network.

28. A system as claimed in any one of claims 24 - 27, wherein said gateway node includes second communication means for requesting, if necessary, the digital cellular radio communications network, with which said end user has a subscription, to perform a registration update with respect to said subscription, in order to receive verification parameters associated with said subscription.

29. A system as claimed in any one of claims 16 - 28, wherein said server is a server of a content provider on said Internet Protocol based network.

30. A system as claimed in claim 29, wherein said content provider is either an E-commerce provider, a Voice-over-Internet provider or an Internet Service Provider.

31. A system as claimed in any one of claims 16 - 30, wherein said gateway node is a logical node comprising a number of subnodes among which operations and functionality of said logical node are distributed.

32. A gateway node for providing services on an Internet Protocol based network, to which network a terminal of an end user and a server of a content provider are connected, said terminal being arranged to read an IC card storing subscriber information relating to a subscription with an operator of a digital cellular radio communications network, for example a GSM network, wherein said gateway node interconnects said Internet Protocol based network with either said digital cellular radio communications network or with a network of the same kind

as said digital cellular radio communications network, said node including:

receiving means for receiving a verification request from said server to verify said end user; and

verification means for performing a verification of said subscription stored on said IC card, which card for example is a Subscription Identity Module (SIM) card, in accordance with a verification scheme, for example a GSM authentication scheme, applied by said digital cellular radio communications network.

33. A node as claimed in claim 32, having the features of the node in the system as claimed in any one of the claims 16 - 18, 20, 24 - 28 or 31.

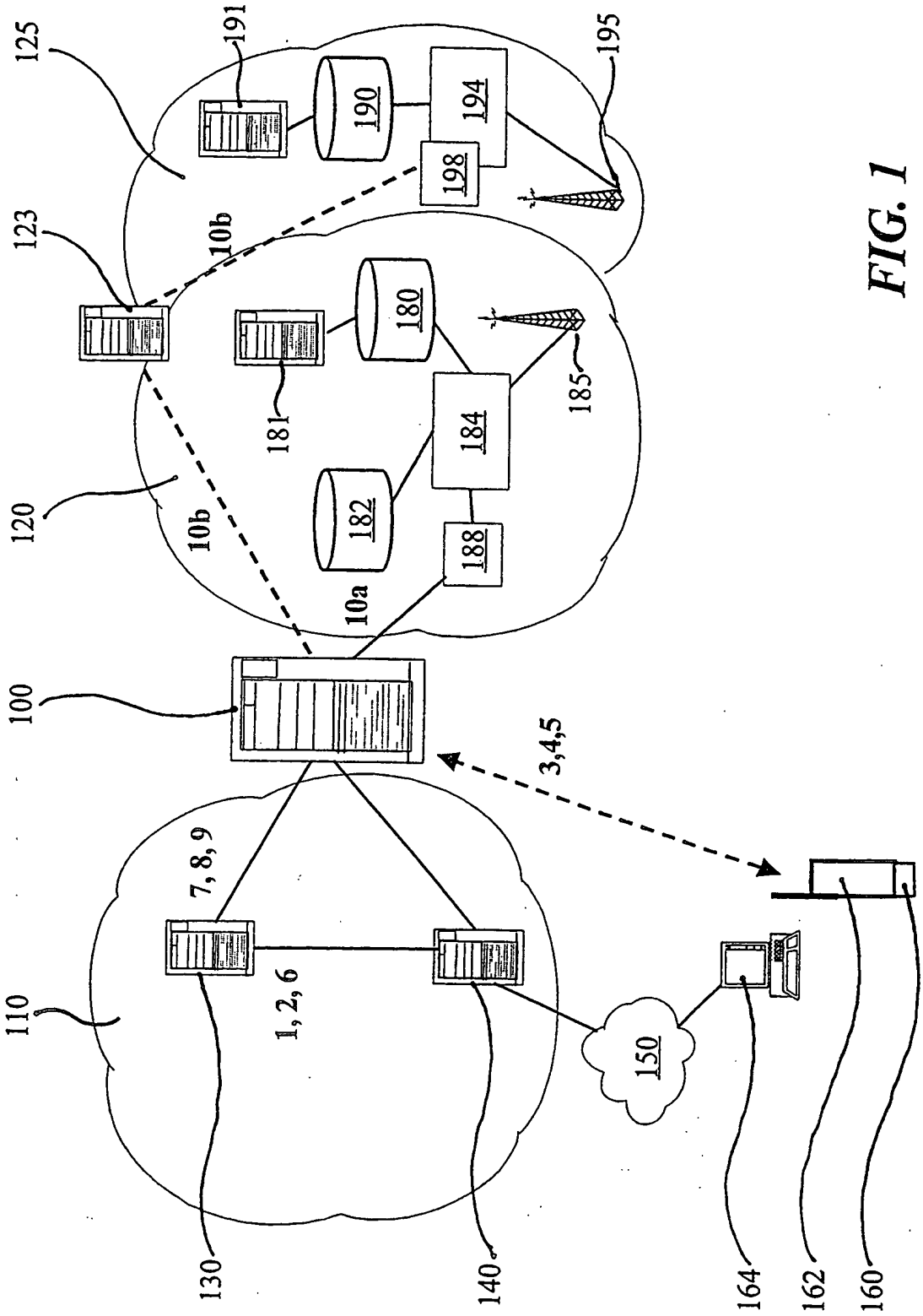

125
191
190
194
195
198
123
10b
180
181
185
184
120
182
188
10a
100
3,4,5
7, 8, 9
110
1, 2, 6
150
130
140
164
162
160

FIG. 1

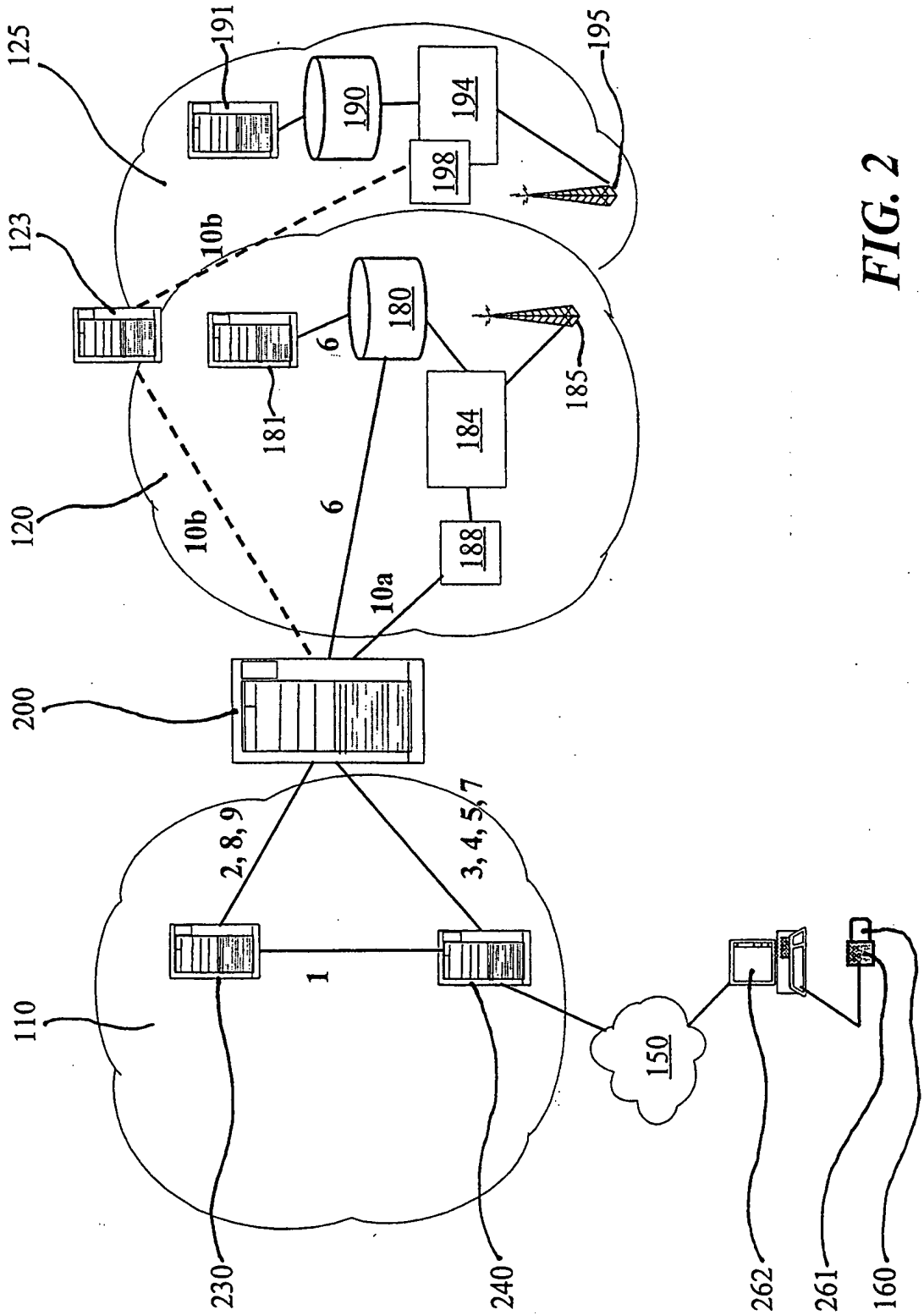


FIG. 2

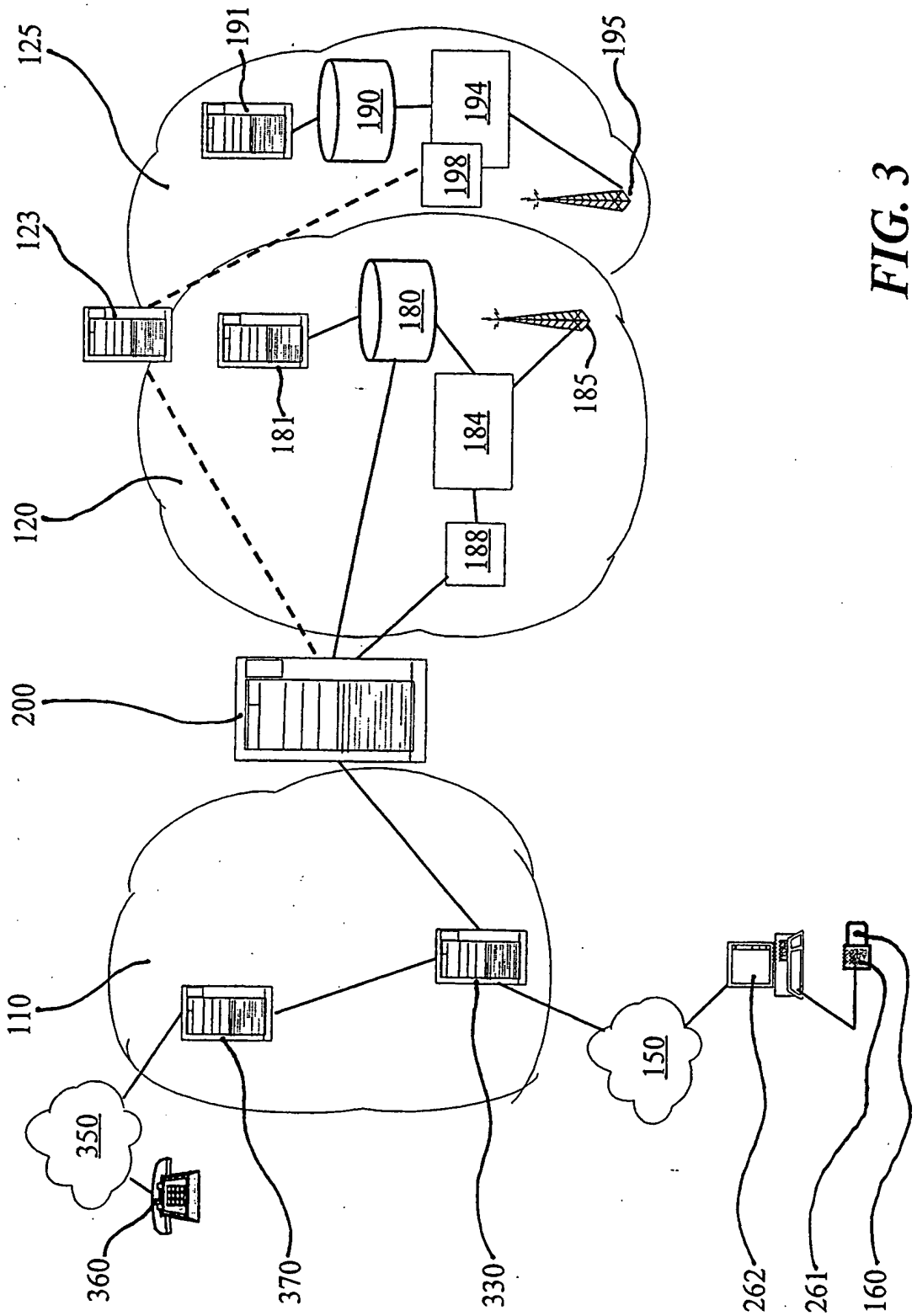

125
191
190
194
195
198
123
180
181
185
184
120
188
200
110
150
350
360
370
330
262
261
160

FIG. 3

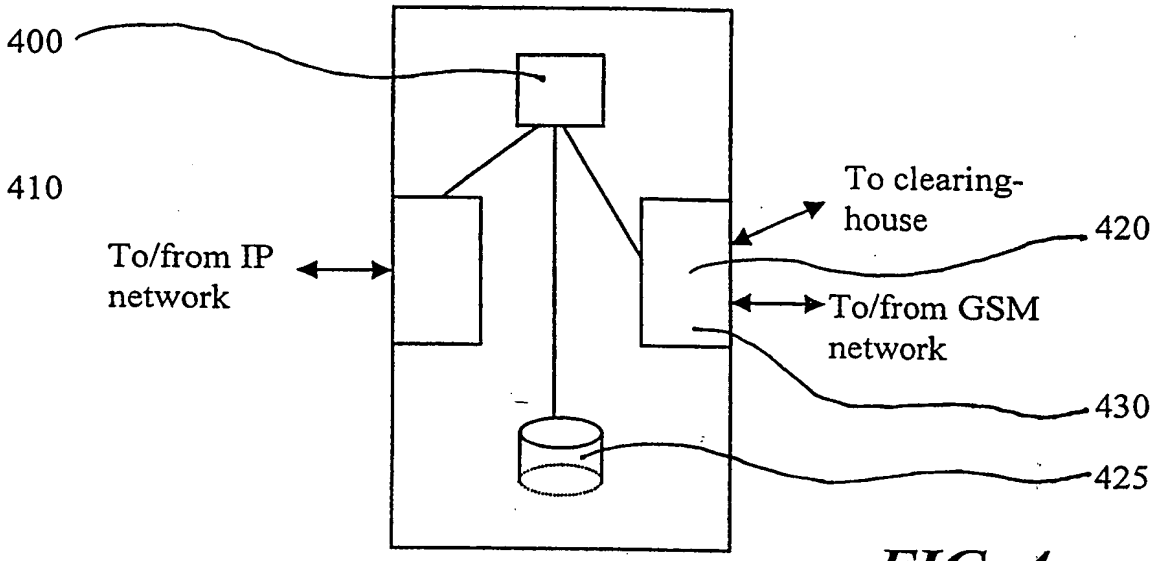


FIG. 4

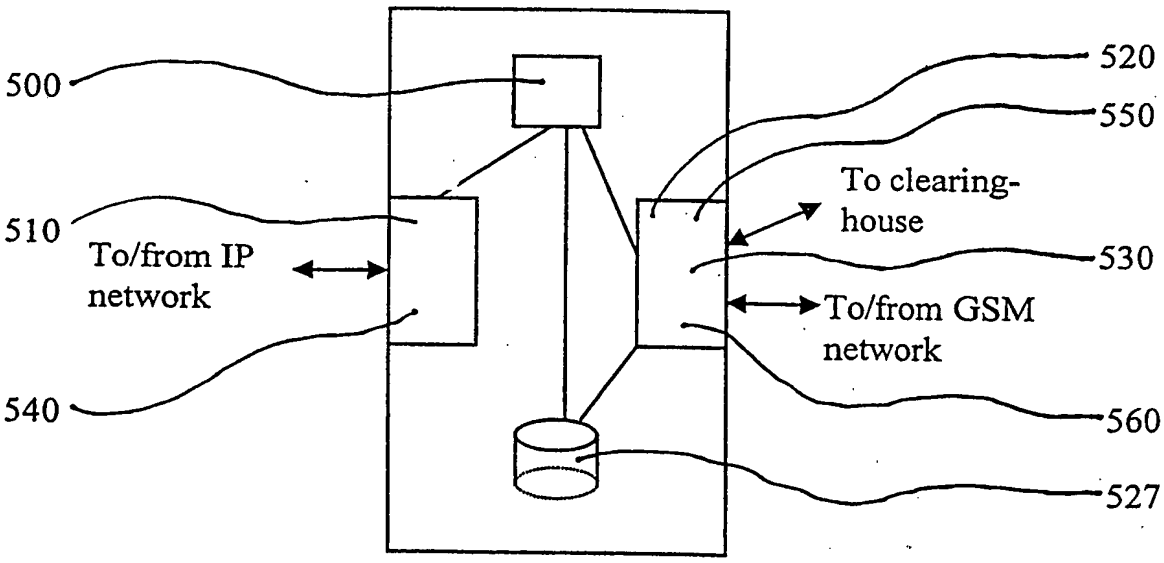


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/00048

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32, H04L 12/14, H04L 12/66
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 9832301 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 23 July 1998 (23.07.98), page 8, line 5 - page 9, line 15; page 12, line 29 - page 16, line 11, figure 1	1,5-15,16, 19-31,32-33
A	Chuah, C., and Spiller, M.D., Infrastructure for a Secure Interface between Wireless and Data Networks (online), December 14, 1998 (retrieved on 1999-10-27). Retrieved from the Internet: <http://www-cad.eecs.berkeley.edu/~mds/classes/cs261/writeup.html>.	1-33

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 June 2000	22 -06- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Patrik BLidefalk/AE Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/SE 00/00048

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9832301 A1	23/07/98	AU 5684698 A	07/08/98
		EP 0953265 A	03/11/99